CLAIMS

What is claimed is:

22. A system for verifying the authenticity of an object comprising:

a signal source;

a first subsystem receiving a first signal from the signal source and providing as output therefrom a first output signal;

a second subsystem receiving a second signal from the signal source and providing as output therefrom a second output signal;

a third subsystem receiving the first and second output signals for comparing the first output signal with the second output signal.

23. The system for verifying the authenticity of an object as set forth in Claim 22 wherein the signal source comprises an optical source.

24. The system for verifying the authenticity of an object as set forth in Claim 22 wherein the first subsystem is an optical subsystem.

25. The system for verifying the authenticity of an object as set forth in Claim 22 wherein the second subsystem is an optical subsystem.

26. The system for verifying the authenticity of an object as set forth in Claim 22 wherein the third subsystem is an optical subsystem.

27. The system for verifying the authenticity of an object as set forth in Claim 23 wherein the optical source is a source of coherent light.

26

28.   The system for verifying the authenticity of an object as set forth in Claim 27 wherein the source of coherent light comprises a laser operative to provide a laser beam to the first and second subsystems.

29.   The system for verifying the authenticity of an object as set forth in Claim 24 wherein the first optical subsystem comprises

a first beam expander for expanding the first signal;

a first collimating lens for collimating the first signal;

a primary image disposed within the path of the first signal;

a random code disposed within the path of the first signal;

a first transforming lens disposed within the path of the first signal;

a filter disposed within the path of the first signal; and

an imaging subsystem for imaging a first reference image comprising the combination of the primary image and the random code.

30.   The system for verifying the authenticity of an object as set forth in Claim 25 wherein the second optical subsystem comprises

a second beam expander for expanding the second signal;

a second collimating lens for collimating the second signal and illuminating a second reference image;

a beam splitter for receiving the collimated second signal and a reference signal from the second reference image; and

a second transforming lens for receiving a signal representative of the second reference image.

27

31.   The system for verifying the authenticity of an object as set forth in Claim 26 wherein the third optical subsystem comprises:

a beam combiner for combining the first and second output signals;

a detector for recording the combined first and second output signals generating thereby a joint power spectrum; and

a signal comparator in signal communication with the detector for comparing the first and second output signals.

32.   The system for verifying the authenticity of an object as set forth in Claim 31 wherein the detector comprises a charge coupled device.

33.   The system for verifying the authenticity of an object as set forth in Claim 31 wherein the comparator comprises:

a nonlinear transfer function generator for applying a *k-th* power law nonlinear transformation to the joint power spectrum; and

a transforming system in signal communication with the nonlinear transfer function generator for performing the correlation of the nonlinearly transformed joint power spectrum; and

a system for analyzing the peaks of the correlation of the nonlinearly transformed joint power spectrum.

34. A method of verifying the authenticity of an object, the method comprising:

encoding a primary image;

convolving the encoded primary image with a random code, generating thereby a first reference image;

transforming the first reference image; and

correlating the first reference image with a second reference image.

35. The method as set forth in Claim 34 wherein encoding the primary image comprises phase encoding the primary image.

36. The method as set forth in Claim 35 wherein phase encoding the primary image comprises phase encoding the primary image according to the equation

$$g(x,y) = exp\{i\pi f(x,y)/Max[f(x,y)]\},$$

where $f(x,y)$ is the primary image, $Max[f(x,y)]$ is the maximum value of $f(x,y)$ and $g(x,y)$ is the phase encoded primary image.

37. The method as set forth in Claim 34 wherein convolving the encoded primary image with a random code comprises convolving the encoded primary image with a random code that is the Fourier transform of a phase-only uniform random distribution.

38. The method as set forth in Claim 34 wherein convolving the encoded primary image with a random code comprises convolving the encoded primary image with a filter that is matched to the random code.

39. The method as set forth in Claim 34 wherein transforming the first reference image comprises Fourier transforming the first reference image.

29

40. The method as set forth in Claim 34 wherein correlating the transformed first reference image with a second reference image comprises generating a phase-only first reference image according to the equation

$$\bar{r}(x,y) = \frac{r(x,y)}{|r(x,y)|} \ ,$$

wherein $r(x,y)$ is the first reference image, $|r(x,y)|$ is the modulus of the first reference image and

$$\bar{r}(x,y)$$

is the phase-only first reference image.

41. The method as set forth in Claim 34 wherein correlating the first transformed reference image with a second reference image comprises transforming the second reference image.

42. The method as set forth in Claim 41 wherein correlating the first transformed reference image with a second reference image comprises generating a joint power spectrum of the first transformed reference image and the second transformed reference image.

30

43. The method as set forth in Claim 42 further comprising:applying a threshold function equal to the sum of the self product terms of the joint power spectrum to joint power spectrum, generating thereby a modified joint power spectrum;applying a *k-th* power law nonlinear transformation to the modified joint power spectrum; and

5   analyzing the peaks of the correlation of the modified joint power spectrum of the first reference image and the second reference image;

wherein the presence of a single peak indicates the authenticity of the object and the presence of no peaks indicates the lack of authenticity of the object.

44. The method as set forth in Claim 43 wherein performing the correlation of the

10   modified joint power spectrum comprises:

inverse Fourier transforming the modified joint power spectrum; and

squaring the modulus of the inverse Fourier transform of the modified joint power spectrum.

45. The method as set forth in Claim 43 wherein *k* lies within the interval

15   between zero and one inclusive.

46. The method as set forth in Claim 40 wherein generating a phase-only reference image includes binarizing the phase-only reference image according to the equation

$$\overline{r_B}(x,y) = \frac{r(x,y)}{|r(x,y)|}$$

where

$$\overline{r}_B (x,y) = \begin{cases} -1 \ \ if \ Re\big[r(x,y)\big] < \ 0, \\ 1 \ if \ Re\big[r(x,y)\big] \ge \ 0 \end{cases}$$

wherein $\overline{r}_B (x,y)$ is the binarized phase-only reference image and

wherein $Re[r(x,y)]$ denotes the real part of $r(x,y)$.

47. The method as set forth in Claim 34 further comprising affixing the second reference image to an object, the authenticity of which is to be verified.

32

48. A method of generating a reference image for verifying the authenticity of an image, the method comprising encoding a primary image;

convolving the encoded primary image with a random code, generating thereby a reference image;

transforming the reference image.

49. The method as set forth in Claim 48 wherein encoding the primary image comprises phase encoding the primary image.

50. The method as set forth in Claim 49 wherein phase encoding the primary image comprises phase encoding the primary image according to the equation

$$g(x,y) = exp\{i\pi f(x,y)/Max[f(x,y)]\},$$

where $f(x,y)$ is the primary image, $Max[f(x,y)]$ is the maximum value of $f(x,y)$ and $g(x,y)$ is the phase encoded primary image.

51. The method as set forth in Claim 48 wherein convolving the encoded primary image with a random code comprises convolving the encoded primary image with a random code that is the Fourier transform of a phase-only uniform random distribution.

52. The method as set forth in Claim 51 wherein convolving the encoded primary image with a random code comprises convolving the encoded primary image with a filter that is matched to the random code.

53. The method as set forth in Claim 48 wherein transforming the reference image comprises Fourier transforming the reference image.

54. A method of encrypting a set of data, the method comprising:

encoding the set of data with a first encryption key;

transforming the set of data encoded with the first encryption key;

with a second encryption key, encoding the transformation of the set of
data encoded with the first encryption key; and

5

transforming the encoded transformation of the set of data encoded with
the first encryption key generating thereby an encrypted set of data.

55. The method as set forth in Claim 54 wherein the set of data includes an
optical image, a transparency, a binarized image, a one dimensional set of data, a two
dimensional set of data, a multi-dimensional set of data, and electrical signal or an optical
10   signal.

56. The method as set forth in Claim 54 further comprising acquiring the set of
encrypted data in a medium responsive to an optical signal, a transparency, a binarized
image, a one dimensional set of data, a two dimensional set of data, a multi-dimensional
15   set of data an electrical signal or an optical signal.

57. The method as set forth in Claim 56 wherein acquiring the set of encrypted
data comprises combining the set of encrypted data with a reference set of data.

58. The method as set forth in Claim 57 wherein combining the set of encrypted
data with a reference set of data includes holographically combining the set of encrypted
20   data with a reference set of data.

59. The method as set forth in Claim 58 wherein the reference set of data
comprises a binarized image, a one dimensional set of data, a two dimensional set of data,
a multi-dimensional set of data an electrical signal or an optical signal.

60. A method of encrypting and decrypting a set of data, the method comprising:

encoding the set of data with a first encryption key;

transforming the set of data encoded with the first encryption key;

with a second encryption key, encoding the transformation of the set of data encoded with the first encryption key;

transforming the encoded transformation of the set of data encoded with the first encryption key generating thereby an encrypted set of data; and

decrypting the encrypted set of data.

61. The method as set forth in Claim 60 wherein the set of data includes an optical image, a transparency, a binarized image, a one dimensional set of data, a two dimensional set of data, a multi-dimensional set of data, and electrical signal or an optical signal.

62. The method as set forth in Claim 40 further comprising acquiring the set of encrypted data in a medium responsive to an optical signal, a transparency, a binarized image, a one dimensional set of data, a two dimensional set of data, a multi-dimensional set of data an electrical signal or an optical signal.

63 The method as set forth in Claim 62 wherein acquiring the set of encrypted data comprises combining the set of encrypted data with a reference set of data.

64. The method as set forth in Claim 63 wherein combining the set of encrypted data with a reference set of data includes holographically combining the set of encrypted data with a reference set of data.

35

65. The method as set forth in Claim 64 wherein the reference set of data comprises a binarized image, a one dimensional set of data, a two dimensional set of data, a multi-dimensional set of data an electrical signal or an optical signal.

66. The method as set forth in Claim 60 wherein decrypting the set of encrypted data comprises:

    acquiring the second encryption key as a hologram;

    combining the encrypted set of data and the second encryption key; and

    transforming the combination of the encrypted set of data and the second encrypted key.

67. The method as set forth in Claim 66 wherein transforming the combination of the set of encrypted data and the reference set of data includes Fourier transforming the combination of the set of encrypted data and the reference set of data.

68. The method as set forth in Claim 54 wherein encoding the set of data with a first encryption key includes multiplying the set of data by the first encryption key.

69. The method as set forth in Claim 54 wherein transforming the set of data encoded with the first encryption key includes Fourier transforming the set of data encoded with the first encryption key.

70. The method as set forth in Claim 54 wherein with a second encryption key, encoding the transformation of the set of data encoded with the first encryption key includes multiplying the second encryption key by the transformation of the set of data encoded with the first encryption key.

36

71. The method as set forth in Claim 54 wherein transforming the encoded transformation of the set of data encoded with the first encryption key includes Fourier transforming the encoded transformation of the set of data encoded with the first encryption key.

72. A system for encrypting a set of data, the system comprising:

a signal source;

a first subsystem receiving a first signal from the signal source and providing as out therefrom a first output signal;

a second subsystem receiving a second signal from the signal source and providing as output therefrom a second output signal;

a third subsystem for combining the first and second signal output.

a fourth subsystem for acquiring the set of encrypted data.

73. The system as set forth in Claim 72 wherein the signal source is comprises an optical source.

74. The system as set forth in Claim 73 wherein the optical source comprises a coherent source.

75. The system as set forth in Claim 74 wherein the first subsystem comprises:

a spatial filter disposed within the path of the coherent source;

a collimating lens disposed within the path of the coherent source; and

a beam splitter disposed within the path of the coherent source for dividing the coherent source into a first signal and a second signal.

37

76. The system as set forth in Claim 74 wherein the second subsystem comprises:

a first transforming lens disposed within the first signal path;

a second transforming lens disposed within the first signal path; and

a beam redirection apparatus for redirecting the first signal path.

77. The system as set forth in Claim 74 wherein the third subsystem comprises:

a beam redirection apparatus for redirecting the second signal path;

a phase mask disposed within the second signal path;

a third transforming lens disposed within the second signal path;

a fourth transforming lens disposed within the second signal path; and

a fifth transforming lens disposed within the second signal path.

78. The system as set forth in Claim 74 wherein the fourth subsystem comprises:

a beam combiner for combining the first and second signals; and

a recording apparatus for recording the combination of the first and second signals.

79. The system as set forth in Claim 29 wherein the filter comprises a spatial filter matched to the random code.

80. The system as set forth in Claim 29 wherein the primary image and the random code are disposed at a first focal plane of the first transforming lens.

81. The system as set forth in Claim 29 wherein the filter is disposed at a second focal plane of the first transforming lens.

82. The system as set forth in Claim 30 wherein the reference image is affixed to the object, the authenticity of which is to be verified.

83. The method as set forth in Claim 66 wherein combining the encrypted set of data and the second encryption key includes multiplying the encrypted set of data and the second encryption key.

5

39